



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,794	08/16/2001	William L. Jones	002.0221.01	3670

7590 09/19/2005
ZILKA-KOTAB, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/931,794

Applicant(s)

JONES ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) See Continuation Sheet is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) See Continuation Sheet is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Continuation of Disposition of Claims:

Claims pending in the application are 1,3-7,9,10,12-16,18-20,22-24,26,28-30,32,33,36,37,39,42,43,45,46,50,51,55-57,59,61,63,65,66,69 and 72-78.

Claims rejected are 1,3-7,9,10,12-16,18-20,22-24,26,28-30,32,33,36,37,39,42,43,45,46,50,51,55-57,59,61,63,65,66,69 and 72-78.

Art Unit: 2137

DETAILED ACTION

Claims 1,3-7,9-10,12-16,18-20,22-24,26,28-30,32-33,36-37,39,42-43,45-46,50-51,55-57,59,61,63,65-66,69, and 72-78 have been considered. The terminal disclaimer has been entered and overcomes the double patenting rejection. Regarding the 103(a) rejection, the examiner disagrees with the applicant's remarks and maintains the previous rejection.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/30/05 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1,3-7,9-10,12-16,18-20,22-24,26,28-30,32-33,36-37,39,42-43,45-46,50-51,55-57,59,61,63,65-66,69, and 72-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg, U.S. Patent No. 6,587,949, in view of Matsushita, European Patent Application No. 00309498.4, in further view of Friedman, U.S. Patent No. 5,499,294.

Art Unit: 2137

As per claims 1,2,10,11,20-21,26-27,33-34,39-40,46,50-51,57,61,66,69, and 74-77, the applicant describes a system with the following limitations which are met by Steinberg in view of Matsushita in further view of Friedman:

5 a) recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium (Steinberg: Col 2, lines 22-34);

b) a frame buffer dividing the intercepted substantially continuous video signal into individual frames during recording, each individual frame storing a fixed amount of data in digital form, and combining decrypted frames into a substantially continuous video signal during playback (Matsushita: Col 3, lines 25-52);

10 c) a processor encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames during recording and retrieving the encrypted frames and decrypting each encrypted frame using a decryption cryptographic key during playback (Matsushita: Col 3, lines 25-52; Steinberg: Col 4, lines 4-11);

15 d) reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium (Matsushita: Col 3, lines 25-52);

e) a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key, where the removable storage medium is removable with respect to the transportable storage medium (Steinberg: Col 4, lines 4-11);

20 f) an authentication module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key; storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash (Friedman: Col 4, line 63 to Col 5, line 14; Col 10, lines 8-15);

25

Steinberg discloses a cryptographic system for legacy systems in which a transportable storage medium, such as a memory card, is inserted into a video recorder. When the video recorder sends video

Art Unit: 2137

data to the memory card for storage, the memory card intercepts the data and performs authentication and encryption on the data before it is stored. Steinberg also discloses the use of a removable storage medium (16 of Fig 1), which can be any system capable of receiving data. After recording takes place, the transportable storage medium is taken to the removable storage medium and the two devices are
5 connected through a cord (Col 3, lines 59-61). The two devices which are connected together by a cord are removable with respect to each other. Thus, item 16 of Fig 1 is removable with respect to the transportable storage medium, item 10 of Fig 1. Also, the removable storage medium stores a cryptographic key for use in decrypting the encrypted content. (Col 6, lines 47-48; Col 6, lines 58-59).

Steinberg does not disclose that data is divided into frames and encrypted frame by frame. This
10 particular encryption technique is disclosed by Matsushita. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Matsushita with those of Steinberg because doing so allows the data to be encrypted in an organized manner in accordance with the common style of processing video data in frames.

Steinberg in view of Matsushita do not disclose the use of computing a hash as authentication
15 data from at least one frame. Friedman discloses a similar process whereby hashes are made on individual frames. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Friedman with those of Steinberg and have a hash computed on an individual frame because computing a hash on the authentication data provides a means to verify the integrity of the framed data.

20 As per claims 3,5-7,12,14-16,22-24,28-30,36-37,42-43,55,59, and 63, the applicant describes the method of claim 2 (etc), which is met by Steinberg in view of Matsushita in further view of Friedman, with the following limitation which is met by Friedman:

Further comprising an asymmetric cryptographic key pair comprising a private key corresponding
25 to the encryption cryptographic key and a public key corresponding to the encryption decryption key (Friedman: Col 2, lines 2-59);

The use of both symmetric and asymmetric cryptography is disclosed by Friedman.

As per claims 4 and 13, the applicant describes the system of claim 1 (etc), which is met by Steinberg in view of Matsushita, with the following limitation which is also met by Steinberg:

5 A validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames (Steinberg: Col 5, lines 52-57).

As per claims 9 and 18, the applicant describes the system of claim 1, with the following limitation which is also met by Steinberg:

10 A set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key (Col 4, lines 4-11).

As per claims 19,32,45,56,65, and 72, the applicant describes the method according to claim 10 (etc), which is met by Steinberg in view of Matsushita in further view of Friedman, with the following limitation which is met by Steinberg:

15 A computer-readable storage medium holding code (Steinberg: Col 2, lines 3-7).

As per claim 73, the applicant describes the system of claim 1, which is met by Steinberg in view of Matsushita, with the following limitation which is met by Steinberg:

20 Wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys (Steinberg: Col 3, lines 59-61; Col 4, lines 4-11);

The connector is the cord.

25 Claim 78 is rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg in view of Matsushita in further view of Friedman in further view of Yuen, U.S. Patent No. 5,621,579.

Art Unit: 2137

As per claim 78, the applicant describes the system of claim 1, which is met by Steinberg in view of Matsushita in further view of Friedman, with the following limitation which is met by Yuen:

Wherein the removable storage medium is removably coupled to a video tape cassette (Yuen: Col 5, lines 11-14).

5 Steinberg in view of Matsushita discloses all the limitations of claim 1. However, Steinberg in view of Matsushita fails to disclose that the transportable storage medium, which is coupled to the removable storage medium, is specifically a video tape cassette.

Yuen discloses the commonly known idea that a video tape cassette can be used to store information recorded from a video recorder. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Yuen with those of Steinberg in view of Matsushita and incorporate the use of a video tape cassette as the transportable storage medium because a video tape cassette is a common storage medium for storing data from a video recorder.

10

Response to Arguments

15 Applicant's arguments, see Remarks, filed 8/30/05, with respect to the double patenting rejection have been fully considered and are persuasive in light of the Terminal Disclaimer filed. The double patenting rejection has been withdrawn.

The applicant's argument with regard to claim 1 and the Steinberg reference has been considered. The applicant argues that Steinberg does not teach that the removable storage medium stores a cryptographic key. The examiner disagrees. The removable storage medium does store a cryptographic key for use in decrypting the encrypted content (Col 6, lines 47-48; 58-59). The examiner fails to see the relevance of the applicant's argument regarding the PCMCIA card since the examiner never indicated the PCMCIA card stores the cryptographic key.

20

25 The applicant's argument with respect to claim 1 and the Friedman reference has also been considered. The applicant argues that the image frames in the Friedman are not being hashed and that

Art Unit: 2137

only the additional information is being hashed to form the digital signature. The examiner disagrees.

The purpose of Friedman's system is to provide a means to authenticate and verify the integrity of image frames. Additional data may be inserted in the frame and the image frame with the additional data is hashed together to produce the signature (Col 4, lines 63-66). The original image file is transmitted with

5 the digital signature. Further, as taught by Friedman, "Any alteration of the original image file transmitted with the digital signature, will result in a mismatch of the two hashes compared" (Col 5, lines 5-8). Since any alteration of the image frame results in a mismatch of the hash, it is clear that the hash is comprised of the image frame. If the digital signature were merely comprised of the additional data and not the image file data as alleged by the applicant, an alteration of the image file would **NOT** result in a hash

10 mismatch. See also (Col 5, lines 56-65).

Conclusion

This action is made non-final.

Any inquiry concerning this communication or earlier communications from the examiner should
15 be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

20 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)
25 at 866-217-9197 (toll-free).


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER